DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 5: Passwords

1. References:

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. AR 380-67, Personnel Security Program, 9 September 1988.

   d. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

   e. DOD Instruction 8500.2, "Information Assurance (IA) Implementation", 6 February 2003.

   f. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

   g. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

   h. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

2. Purpose of Policy. The 4ID automated information systems (AIS), i.e. laptops, desktops, servers, and information transport network (ITN) infrastructures provide the primary automated information infrastructure supporting operational and administrative functions. These systems provide reliable, timely, and direct methods of communicating electronically and storing information essential to daily operations. Technical controls shall be adopted to ensure that access to information resources is limited to authorized personnel.

3. Applicability: This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities:

   a. 4ID Commanders/Directors and owners of AIS: Owners of information systems are responsible for ensuring that Information Assurance (IA) solutions are in place to safeguard information resources for which they are responsible. It is the responsibility of Commanders/Directors to ensure that these solutions are used.

   b. 4ID Information Assurance Network Manager (IANM): The IANM will audit (scan) 4ID IP address space a minimum of twice a year to ensure compliance with the Password Policy. Through the audit process, identify and implement enhancements that can be made to increase the effectiveness in administering this policy.

   c. AIS Users: Users are responsible for creating passwords that conform to this policy, keeping passwords private, and reporting changes in their user status (e.g., transferred, access level changes, etc.). Suspected security violations shall be reported to the IANM/IASO, who shall

investigate the alleged violation and coordinate a response with the appropriate System Administrator, or IA Manager.

5. Policy:

a. Password Length and Composition: A password will have a minimum length of 10 characters including at least two numbers, two special characters (a shifted number such as !, @, #, $, %, etc), two upper case alphabetic characters, and two lower case alphabetic characters. AIS will be configured to force compliance with this composition rule where possible. An exception to this composition rule shall only be made for systems that do not support this password convention. In that event, variance shall be authorized and confirmed in writing by the responsible IASO. Passwords will not include references such as social security numbers, birthdays, user IDs, names, slang, military acronyms, call signs, dictionary words, consecutive or repetitive characters, system identification, or anything easily guessed.

b. Initial System Passwords: Many systems come from the vendor with a number of standard user IDs (e.g., SYSTEM, TEST, ADMINISTRATOR, etc.) already enrolled in the system. The System Administrator (SA) shall change the default vendor-supplied passwords for all user IDs before connecting the AIS to the network or allowing the general user population to access the system.

c. Initial Password Assignment: The System Administrator or IASO is responsible for generating and assigning the initial password for each user ID. The user shall then be informed of this password. Upon initial login, the user shall be required to immediately change the password.

d. Nullifying Exposure: The password generated by the System Administrator or IASO shall be forwarded to the user by secure means, with instructions that upon initial login the user shall change the password. Within the system itself, the user ID shall be identified as having an expired password, or other similar mechanism, which will require the user to change the password by the usual procedure before receiving authorization to access the system.

e. Password Change Authorization: The System Administrator or IASO shall be permitted to change the password of any user at any time if he/she suspects any breeches in security. The System Administrator or IASO shall inform the user, responsible Information Assurance Manager (IAM) in such circumstances, but is not required to do so prior to the change. In the event of a security breech, the user shall call his/her system administrator or IASO, who shall set a new password as done with initial password assignment.

f. Privileged Logins: Access to privileged logins, such as root/administrator, shall be limited to the designated system administrator(s). Other users that require privileged logins shall log in under their own user ID, then through the use of root equivalence protocols may be authorized access to a subset of super user command privileges (by using commands like "sudo"). This assignment of privileged access shall be restricted to the minimum number of individuals necessary to effectively provide support to users or for system development, test, and production services. Users with escalated privileges (e.g. system administrators) shall use separate "administrative" accounts to perform administrative functions.

g. Root Password: The root/administrator account password for each system shall be recorded on paper in a memo and forwarded in a sealed envelope, or written and sent by encrypted means, to the AIS IASO. The IASO shall place the envelope or printed email message in a locked container with restricted access. If the system root/administrator password is changed, the System Administrator shall update the memo immediately.

h. Individual Accountability: It will be considered a security violation when two or more people know the password for a System Administrator/IASO configurable user ID, except in the case

when the System Administrator/IASO is the other person and the user ID is identified by the system as having a newly created account or an expired password. Individual accountability and audit-ability are critical system security components.

i. Group IDs: Group IDs or scripts may be used to allow classification of users based on needs and privileges to be assigned. However, there shall be no user IDs used by more than one person to access data, thus circumventing individual user accountability. Establishing generic "temp," "guest" or other similar accounts for use by multiple or temporary users is strictly prohibited.

j. Account Deactivation and Deletion: User accounts will be disabled immediately by the System Administrator upon notification of an individual's voluntary or involuntary termination of employment, transfer or retirement. The supporting IMO will be notified of the action. Disabled user accounts will be deleted after 90 days unless the supporting IMO has an approved exception from the IASO for the AIS. An exception must clearly state the justification for the action and the new date for account deletion.

k. Changing Passwords: There shall be a maximum lifetime for all passwords. To protect against potential threats, it is required that a password be changed every 150 days at a minimum. For those users with escalated privileges (e.g. systems administrators), passwords shall be changed every 89 days at a minimum.

l. Expired Password: A password shall be invalidated at the end of its maximum lifetime. At a pre-determined period of time prior to the expiration of a password's lifetime, the user ID it is employed with shall be notified by the system that the password will "expire" in *'x'* days. A user who logs in with an ID having an expired password shall be required to change the password for that user ID before further access to the system is permitted. If the password is not changed before the end of its maximum lifetime, the user ID it is employed with shall be identified by the system as "locked." No login shall be permitted to a locked user ID until the System Administrator/IASO has been able to unlock the user ID by changing the password for that user ID. Then, following the same rules that apply to the initial password entry, a user may again access the system.

m. Change Authorization: Consistent with the password privacy goal, users (other than the system administrators, IASO) shall be permitted to change only their own passwords. To ensure compliance, users are required to enter their old password as part of the password changing procedure.

n. Login to a Connected System: Users shall be required to authenticate their identities at login by supplying their user ID along with their password. Privileged logins to the system, such as "root/administrator" logins, shall not be directly accessed in order for system logging to be effective. Instead, system users must use their own uniquely identifiable account, and if required to perform their job function, enabling super-user equivalence using commands like "su". It is recommended that some form of trusted identification forwarding be used between hosts when users connect to other AIS in the network. When trusted identification forwarding is not used, a remote host shall require the user's ID and password when logging in through a network connection.

o. Remembering Passwords: It is recommended that users memorize their passwords and not write them on any medium. If passwords must be written, they shall be protected in a manner consistent with the damage that could be caused by their compromise. A suggested method is to write the password and seal it in an envelope with the seal signed by the user selecting the password. Store the envelope in a secure location, such as a safe or locking file, to be accessed when necessary.

p. Password Validation and Audit: The IANM shall ensure compliance with password security requirements at least every 6 months. Password integrity shall be verified through the use of password checking routines and/or scanners.

6. Non-compliance:

a. If an account is found to have a non-compliant password, the IANM will direct the SA to immediately change it, following initial password procedures. In those instances where the SA is unable to apply an affected change, the IANM will direct the network administrators to block access to the effected AIS at the nearest router/firewall. The block will remain in place until a compliant password is applied by the SA and verified by the IANM.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding